Posudek oponenta diplomové práce

Bc. Tomáše Tománka

„Aplikovaná kryptologie v internetové komunikaci"

Předložená diplomová práce se zabývá mimořádně aktuálním tématem. Text je kromě předmluvy, úvodu a závěru adekvátně strukturován do čtyř hlavních kapitol představujících nejdříve teoretický základ práce (kap. 2 a 3), dále velmi pěkně a podrobně popsané aplikace na internetu (kap. 4) a nakonec případovou studii týkající se mobilní sítě.

Celkově dobrá grafická úroveň předložené práce je, bohužel, poznamenána nedůsledným používáním hierarchie nadpisů. Občas dokonce v textu chybí číslování subkapitol podle obsahu – namátkou 3.3.3 na str. 37 a v celé kapitole 5. Ani vlastní obsah na str. 1-2 není formálně úplně v pořádku.

Z jazykového hlediska jsem v práci nenalezl významnější nedostatky, pouze ojedinělé překlepy: na 4.ř. textu kap.4 „přibily", na 10.ř. zdola str. 104 „dotisk", na 5.ř. zdola str. 93 „klokovací", na 8. ř. str. 99 „klokování". K diskusi je samozřejmě český výraz pro „hash" – domnívám se, že více než „haš", použitý v předložené práci, se zavádí „heš". Za nevhodné považuji české vyjádření anglické zkratky GSM na str. 83 (zvláště při srovnání s touto položkou v seznamu zkratek na str. 114). Vysvětlení zkratky AES na str. 26 a v seznamu na str. 113 je shodné, avšak na str. 26 se píše také o American Encryption Standard – co je správně?

Co se týče použité literatury, domnívám se, že její rozsah (69 položek) svědčí o dobré orientaci v tématu a důkladné přípravě diplomové práce (je však nutno podotknout, že 28 položek jsou odkazy na Wikipedii). Množství doslovných citací v textu je adekvátně vyznačeno s odkazy na prameny.

Z obsahového a terminologického hlediska mám k práci několik připomínek:

První se týká výrazů „logická funkce XOR" (str. 19), „sčítačka mod-2" (str. 22), „bitová nonekvivalence" (str.33). Není to totéž? Autor v práci na používání jednotného termínu rezignoval, nicméně vzhledem k významu této funkce bych navrhl tuto otázku k diskusi při obhajobě.

Popis Diffie-Hellmanova algoritmu na str. 34-35 není zcela jasný. Předposlední řádek str. 34 by měl být pro přesnost doplněn slovy „existuje

k takové, že". Hodnoty veřejných klíčů by na str. 35 měly být označeny *A*, *B* tak, aby bylo zřejmé, s čím se po výměně počítá.

V popisu RSA na str. 36 (a též v závěru na str. 102) se chybně uvádí, že bezpečnost RSA se opírá o obtížnou faktorizaci velmi vysokých prvočísel. Doufám, že to při obhajobě bude uvedeno na pravou míru.

Úvodní výklad k hašovacím funkcím není dobře uspořádán (zřejmě z důvodu nedůsledné kompilace z více pramenů). Vysvětlení vlastností uvedených na str. 38 následuje (bez odkazu) až na str. 41, vysvětlení „narozeninového paradoxu" vůbec chybí (očekávám, že bude podáno aspoň při obhajobě). Není jasný obr. 13 – je uvedený Input celý, nebo jde pouze o jeho měnící se část? Liší se „heslo" (str. 41) a „zpráva", „vstup" (str. 42)? V jakém vztahu k předchozím vlastnostem jsou body 1. a 2. na str. 43?

Některá matematická značení nejsou zcela správně, např. na str. 37 mají zřejmě na levé straně rovností být malá písmena; „jisté Galoisovo těleso" na str. 81 jistě není GF(2128).

V závěru na str. 101 dole je matoucí formulace „V případě nasazení symetrické kryptografie používají všechny komunikující strany stejný klíč pro šifrování i dešifrování zpráv", správně je tato záležitost osvětlena např. na str. 17.

Uvedené připomínky k práci nepovažuji za zásadní. Předložená diplomová práce prokazuje široký přehled autora a rozsáhlé znalosti týkající se role kryptografie v digitální komunikaci. Obtížné téma je fundovaně zpracováno na základě nejnovější literatury a odborný text je doplněn i praktickými ukázkami. Přínosná je konkrétní případová studie. Zvláště oceňuji závěr práce, který je velmi výstižným shrnutím celé problematiky.

Autor splnil zadání diplomové práce a v některých místech je i překročil. Doporučuji práci k obhajobě a navrhuji známku velmi dobře, nebo výborně na základě výsledku obhajoby.

V Praze dne 12.5.2008

Doc. RNDr. Jiří Ivánek, CSc.